

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)INFO. ASSOCIATED WITH INTHESUN1313@GMAIL.COM;
ALEX.FRANGA75@GMAIL.COM;
BMLAKE12345@GMAIL.COM;
BANANAMANN666@GMAIL.COM;
ANTOCHEAMZ@GMAIL.COM; ANTOCHE@MAIL.COM

Case No.

1:18MJ-728

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A.

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

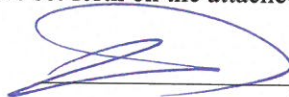
The search is related to a violation of:

Code Section
 18 U.S.C. Sections 1030,
 1343, 1344

Offense Description
 Computer fraud, wire fraud, bank fraud

The application is based on these facts:
 See attached affidavit

- ☐ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Special Agent Tae Dempsey, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 12/7/18City and state: Cincinnati, OH


Judge's signature

Hon. Karen L. Litkovitz, U.S.M.J.

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH

inthesun1313@gmail.com
alex.franga75@gmail.com
bmlake12345@gmail.com
bananamann666@gmail.com
antocheamz@gmail.com

that are stored at premises controlled by
Google, Inc., 1600 Amphitheatre Parkway,
Mountain View, CA 94043

and

antoche@mail.com

that is stored at premises controlled by 1&1
Mail & Media, Inc., 701 Lee Road, Suite 300,
Chesterbrook, PA 19087

Case No.

1:18MJ-728

Filed Under Seal

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Tae Dempsey, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises controlled by 1) Google, Inc., headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043 and 2) 1&1 Mail & Media, Inc., headquartered at 701 Lee Road, Suite 300, Chesterbrook, PA 19087 (the "PROVIDERS"). The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under

18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the PROVIDERS to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been since September 2015. Prior to my employment at the Federal Bureau of Investigation, I was employed for five years as a Vice President and Information Security Officer at a major global bank in the Financial Services sector. While employed by the Federal Bureau of Investigation, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, child pornography, money laundering, and credit card fraud. I have gained experience through training at the Federal Bureau of Investigation and everyday work relating to conducting these types of investigations. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. This investigation pertains to the theft of over \$106,000 from Fifth Third Bank ("FIFTH THIRD") ATMs in Illinois, Michigan, and Ohio. FIFTH THIRD is a federally insured financial institution that is headquartered in Cincinnati, Ohio, which is in the Southern District of Ohio.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1030,

1343, and 1344, among other offenses, have been committed by persons known and unknown. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

7. I have spoken with employees of FIFTH THIRD, as well as reviewed documents prepared by FIFTH THIRD employees, and from those conversations and that review, I have learned, among other things, the following:

a. In May 2018, FIFTH THIRD detected fraudulent activity originating from their mobile banking feature known as “cardless ATM”. Cardless ATM allows customers to withdraw money from a FIFTH THIRD ATM using only their mobile device and the FIFTH THIRD mobile banking application. Customers are not currently able to use this feature at another bank’s ATM. This eliminates the need for a physical card to withdraw cash from a FIFTH THIRD ATM.

b. Upon further investigation, FIFTH THIRD found that an unknown actor had compromised the usernames and passwords, one-time passcodes, and PIN numbers for approximately 125 of their customers. A significant percentage of these customers reside in Cincinnati and the surrounding areas.

c. Based on conversations FIFTH THIRD employees had with affected customers, FIFTH THIRD discovered that affected customers received phishing messages via text message indicating that their accounts were locked. The text messages contained a link to unlock their accounts and led customers to a website that mimicked the legitimate FIFTH THIRD website. The website required customers to enter the account credentials in order to unlock their accounts.

d. After compromising the customer accounts, the unknown actor successfully cashed out approximately \$68,000 in total from 17 ATMs in Illinois, Michigan, and Ohio in less than two weeks through the cardless ATM function. FIFTH THIRD obtained photographic images from those ATM locations. At each location, the unknown actor was wearing a hat and sunglasses to disguise his identity.

e. On or about October 3, 2018, FIFTH THIRD started to receive complaints that customers were receiving phishing messages via text message indicating that their accounts were locked. The text messages contained a link to unlock their accounts and led customers to a website that mimicked the legitimate FIFTH THIRD website. The website required customers to enter the account credentials in order to unlock their accounts.

f. On or about October 10, 2018, FIFTH THIRD detected fraudulent activity originating from their cardless ATM function. Specifically, FIFTH THIRD observed cash withdrawals from ATMs using the cardless ATM application that triggered internal fraud rules. FIFTH THIRD identified two individuals ("Individual-1" and "Individual-2") conducting the fraudulent activity at ATM locations in the Cincinnati metropolitan area.

g. On or about October 15, 2018, FIFTH THIRD started to receive additional complaints that customers were receiving phishing messages via text message indicating that their accounts were locked. The text messages contained a link to unlock their accounts and led

customers to a website that mimicked the legitimate FIFTH THIRD website. The website required customers to enter the account credentials in order to unlock their accounts.

h. On or about October 17, 2018, FIFTH THIRD detected activity involving their cardless ATM function that again triggered internal fraud rules. FIFTH THIRD identified an individual ("Individual-3") who used his personal device to access or attempt to access multiple FIFTH THIRD customer accounts using the cardless ATM function. Some of those transactions were attempted at an ATM in Fairlawn, Ohio, which is in the Northern District of Ohio.

i. On or about October 19, 2018, FIFTH THIRD detected activity involving their cardless ATM function that again triggered internal fraud rules. FIFTH THIRD identified an individual ("Individual-4") who used his personal device to access or attempt to access multiple FIFTH THIRD customer accounts using the cardless ATM function. None of the customer accounts were in Individual-4's name. Some of those transactions were attempted at an ATM location in Blue Ash, Ohio, which is in the Southern District of Ohio.

8. On or about October 10, 2018, law enforcement located and arrested Individual-1 in Cincinnati, Ohio. I have spoken with members of the Cincinnati Police Department ("CPD") and reviewed documents they prepared, and from those conversations, I have learned, among other things, the following:

a. CPD seized over \$12,000 in cash found on Individual-1 and numerous receipts showing cash withdrawals from FIFTH THIRD ATMs.

b. CPD seized multiple identification documents from Individual-1. The identification documents had different names, but the same photo of Individual-1.

c. CPD seized paperwork from Individual-1 that appeared to be a work resume. The resume had a name that matched one the aforementioned identification documents. The resume listed Individual-1's email address **alex.franga75@gmail.com**.

d. On or about October 10, 2018, law enforcement located and arrested Individual-2 West Chester, Ohio. I have spoken with members of the West Chester Police Department ("WCPD") and reviewed documents they prepared, and from those conversations, I have learned, among other things, the following:

e. WCPD seized over \$700 in cash found on Individual-2.

f. WCPD seized Individual-2's vehicle ("Vehicle-1").

9. On or about October 12, 2018, law enforcement executed a search warrant on Vehicle-1. Law enforcement seized, among other items, the following from Vehicle-1:

a. Over \$28,000 in cash and numerous receipts for cash transactions.

b. A ledger of cash transactions and transfers.

c. Other receipts for transactions, among which, was a receipt that showed Individual-2's name and contact information. The receipt also listed **inthesun1313@gmail.com** as Individual-2's email address.

10. On or about October 17, 2018, law enforcement located and arrested Individual-3 in Fairlawn, Ohio. I have spoken with members of the Fairlawn Police Department ("FPD") and reviewed documents they prepared, and from those conversations, I have learned, among other things, the following:

a. FPD seized, among other items, \$2,400 in cash, bank cards, and three phones.

b. FPD located and subsequently conducted an inventory search of Individual-3's rental vehicle. Individual-3 provided the email address **bmlake12345@gmail.com** on the rental vehicle contract.

11. On or about October 19, 2018, law enforcement located and arrested Individual-4 in Blue Ash, Ohio. I have spoken with members of the Blue Ash Police Department ("BAPD") and reviewed documents they prepared, and from those conversations, I have learned, among other things, the following:

a. BAPD seized, among other items, over \$3,600 in cash found on Individual-4, a receipt showing a cash withdrawal from a FIFTH THIRD ATM, a Wells Fargo account number, and a Samsung phone ("Device-1") from Individual-4.

b. BAPD later identified Individual-4's hotel room ("Hotel-1") in Sharonville, Ohio and obtained a search warrant. According to hotel records, no other guests were registered to stay in Hotel-1.

c. BAPD seized, among other items, over \$3,000 in cash and a Dell laptop ("Device-2") from Hotel-1.

12. On or about October 22, 2018, law enforcement obtained and executed a search warrant for Device-1 and Device-2. From the review of these devices, law enforcement has learned, among other things:

a. Device-1 was an Android phone that was setup to use and access the email address **bananamann666@gmail.com**.

b. Device-2 was a laptop that had a text file saved inside of the "Desktop" folder named "pass.txt". This file contained the email addresses **antoche@mail.com** and **antocheamz@gmail.com**.

13. On or about November 7, 2018, I received documents from Wells Fargo regarding the bank account for Individual-4. I have reviewed those documents and have learned, among other things, the following:

a. Individual-4 provided the email address **antoche@mail.com** when opening the account on November 10, 2017.

14. Based on my training and experience, I know that individuals frequently communicate to each other over digital channels, such as email. I also know that individuals often provide their personal email addresses to businesses to receive electronic receipts or order confirmations for products and services such as rental cars, airline tickets, internet services, or other purchases that could be used in furtherance of criminal activities.

15. On or about October 17, 2018, I served a preservation request for **inthesun1313@gmail.com**.

16. On or about October 25, 2018, I served a preservation request for **alex.franga75@gmail.com** and **bananamann666@gmail.com**.

17. In general, an email that is sent to an email subscriber is stored in the subscriber's "mail box" on the PROVIDER's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on the PROVIDER's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the PROVIDER's servers for a certain period of time.

18. On or about November 7, 2018, a Grand Jury in the Southern District of Ohio indicted Individual-1, Individual-2, Individual-3, and Individual-4 for bank fraud, in violation of 18 U.S.C. § 1344(2). *See* 18-CR-138.

BACKGROUND CONCERNING EMAIL

19. In my training and experience, I have learned that the PROVIDERS provide a variety of on-line services, including electronic mail ("email") access, to the public. The PROVIDERS allow subscribers to obtain email accounts at the domain names gmail.com and mail.com, like the email accounts listed in Attachment A. Subscribers obtain an account by registering with the PROVIDERS. During the registration process, the PROVIDERS ask subscribers to provide basic personal information. Therefore, the computers of the PROVIDERS are likely to contain stored electronic communications (including retrieved and unretrieved email for the PROVIDERS subscribers) and information concerning subscribers and their use of PROVIDERS services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the accounts' user or users.

20. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

21. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

22. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

23. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the

information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner’s state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner’s motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

24. Based on the foregoing, I believe there is probable cause that evidence of the aforementioned scheme exists in the target email accounts.

25. Based on the foregoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on the PROVIDERS, who will then compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

26. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,



Tae Dempsey
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on Dec. 7, 2018


HONORABLE KAREN L. LITKOVITZ
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A (GOOGLE)

Property to be Searched

This warrant applies to information associated with the account identified as email accounts controlled by the web-based electronic mail service provider known as Google, Inc., headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The accounts to be searched are **inthesun1313@gmail.com, alex.franga75@gmail.com, bmlake12345@gmail.com, bananamann666@gmail.com, and antocheamz@gmail.com.**

ATTACHMENT A (1&1 MAIL & MEDIA)

Property to be Searched

This warrant applies to information associated with the account identified as email account controlled by the web-based electronic mail service provider known as 1&1 Mail & Media, Inc., headquartered at 701 Lee Road, Suite 300, Chesterbook, PA 19087. The account to be searched is **antoche@mail.com**.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by the PROVIDER

To the extent that the information described in Attachment A is within the possession, custody, or control of the PROVIDER, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to requests made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account from inception to present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the PROVIDER and any person regarding the accounts, including contacts with support services and records of actions taken.

The PROVIDER is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Sections 1030, 1343, and 1344, and occurring since account inception to present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Fraud and related activity in all of its forms, including but not limited to the theft, acquisition, sale, and use of financial institution data such as customer banking account information and customer credentials, identification of co-conspirators or other parties to the fraudulent scheme;
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (e) The identity of the person(s) who communicated with the user ID about matters relating to fraud, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google, and my title is _____.

I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, and they were made by Google as a regular practice; and
- b. such records were generated by Google electronic process or system that produces an accurate result, to wit:
 1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google in a manner to ensure that they are true duplicates of the original records; and
 2. the process or system is regularly verified by Google, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by 1&1 Mail & Media, Inc., and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of 1&1 Mail & Media, Inc. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of 1&1 Mail & Media, Inc., and they were made by 1&1 Mail & Media, Inc. as a regular practice; and

b. such records were generated by 1&1 Mail & Media, Inc. electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of 1&1 Mail & Media, Inc. in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by 1&1 Mail & Media, Inc., and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature